EU data protection policy

Poullet, Yves

Published in:
Computer Law and Security Report

Publication date:
2006

Document Version
Publisher's PDF, also known as Version of record

available at www.sciencedirect.com

SCIENCE DIRECT®

www.compseconline.com/publications/prodclaw.htm

ELSEVIER

Computer Law & Security Report

EU update

EU data protection policy. The Directive 95/46/EC: Ten years after☆

Yves Poullet

University of Namur, Belgium

ABSTRACT

A birthday offers a unique opportunity to remember what has already been achieved along the way and to envisage what comes next, taking into account the lessons of the past. This paper offers some reflections on 10 years of experience with the Data Protection Directive. The following comments are offered in the knowledge that they will not cover the whole picture and may well be considered partial.

1. Introduction

Six points will be taken into consideration in this paper:

- The first one is trivial: after 10 years, where is the promised harmonisation of data protection law?
- The second point is crucial: can we consider that the Data Protection Directive provisions are effective, i.e. that the application of these provisions is being effectively implemented. Five points will be discussed in that respect.
- As regards transborder data flows, different decisions have been taken. Are these decisions appropriate, taking into account the increasing globalisation of the information Society?
- Privacy legislation has to face a technological landscape characterised by rapid and unpredictable evolution. These techniques might jeopardise or enhance our Privacy. To face these new risks, European data protection institutions have developed a techno-legal approach that will be described. The main principle of this attitude might be expressed as follows: "The machine is the problem: the solution is in the machine".
- More and more, Society has to arbitrate between conflicting values insofar as Privacy is merely one value amongst others. I will consider how three conflicts of value have been approached. At issue is how to solve the dilemma of balancing freedom of expression and privacy in the aftermath of 11th September 2001? This will lead to some short reflections on the delicate balance between privacy and other values.
- Last but not least, two important texts adopted since the Directive 95/46/EC, will be taken into consideration. First, the European Human Rights Charter, adopted in 2000, distinguishes clearly between privacy and data protection, envisaging these two concepts as complementary to one another. Secondly, the Directive 2002/58/EC on privacy and communications goes beyond the so-called general Directive and clearly pleads for a third generation of data protection legislation.

Taking these points into account this paper argues for a new role for the Data Protection Authorities, a new cooperative approach and most definitely for innovative solutions.

☆An earlier version of this paper was presented at the 27th International conference of Data Protection Commissioners, Montreux, Switzerland, September 14–16, 2005.

0267-3649/$ – see front matter

doi:10.1016/j.clsr.2006.03.004

2. 10 Years after: where is the promised harmonisation?

The initial dream of the authors[1] of the Directive was to create a uniform market at the European level for personal data ensuring a high level of protection for data subjects. The main principle laid down by Article 1.2 of the Directive is the prohibition on any barriers to the free circulation of personal data. This is despite the fact that Recital 9 recognises possible disparities due to the margin of manoeuvre of the Member States in implementing the Directive. This margin has been largely used by different states in such a way that it becomes difficult to compare the different national Privacy Acts. Certain countries have, more or less, translated the European text as such or with only minor modifications, whereas others have deeply modified the structure, added new definitions or principles or sometimes adopted sectoral or specific legislation. All these considerations create problems for comparison between the different national regimes.

In 2003, eight years after the Directive, a report[2] concerning the implementation of the Directive in the 15 Member States was published in accordance with Article 33 of the Data Protection Directive. It had been foreseen that there would be a report within the three years following implementation of the Directive. This report has been preceded by a quite critical technical report.[3] It underlines many diverging interpretations as regards the fundamental concepts (personal data, data controller, consent, sensitive data...); different approaches as regards delicate questions of applicable law; and the criteria for legitimising the processing and the limitations as regards the data subject's right of access. During the consultation, which preceded the report, multinational companies in particular underlined the complexity of managing compliance[4] across multiple sets of standards, as laid down in national legislation. Certain companies called for a unique European regulation directly applicable in all the countries.

This point of view has been presented as a minority viewpoint. As stated in the Report:

> "In the course of the consultations conducted, few contributors explicitly advocated the modification of the Directive. The most notable exception was the detailed proposals for amendments submitted jointly by Austria, Sweden, Finland and the UK. These proposals for amendments concerned only a small number of provisions (notably Article 4 which determines the applicable law, Article 8 on sensitive data, Article 12 on the right of access, Article 18 on notification and Articles 25 and 26 on transfers to third countries), leaving most of the provisions and all of the principles of the Directive untouched. The Netherlands adhered to these proposals at a later stage."

Notwithstanding these criticisms, the Commission has clearly pleaded against modifying the original text, preferring to pinpoint any misleading interpretations within the diverse national texts.

Beyond that, the Commission has clearly moved towards a "cooperative approach" rather than an aggressive one. Three actions have been proposed. First there will be discussion with the Member States and the Data Protection Authorities to inform the Commission as to any practical difficulties in the relationships between these diverging interpretations and implementations. Second, Member States are to be reminded of their obligation to notify the Commission as to any draft legislation that either partially transposes or fails to transpose the Directive. Third, the report pleads for an immediate and strong association of the candidate countries (the 10 PECO's states (Pays d'Europe Centrale et Orientale – the 10 Member States that joined the EU on 1 May 2004, then candidates for membership)) to the different debates around the Data Protection Directives. A new report is envisaged for 2006 and, in that respect, the report concludes that "the Commission will use its formal powers under Article 226 of the Treaty if this cooperative approach fails to produce the necessary results".

3. Is the Directive effectively applied?

The reflections in this paper commence with a review of the *Privacy Eurobarometers*,[5] published in 2003. This indicates the sensitivity to privacy issues, as well as knowledge of existing

[1] I take the opportunity of this report to recall the important role played by Ulf Bruhänn, head of the Data Protection service at the DG Markt, in the drafting of the Directive, the difficult discussions held for its adoption by the European institutions and the launching up of the first implementation of the text.

[2] First report on the implementation of the Data Protection Directive (95/46/EC). 2003 – 28 pp. – 21 × 29.7 cm, ISBN 92-894-5378-8, No. catalogue KM-51-03-326-EN-C, January 26, 2001 available at: europa.eu.int/comm/justice_home/fsj/privacy/studies/index_en.htm.

[3] D. Korff, "Study on Implementation of Data Protection Directive – Comparative Summary of National laws, by Douwe Korff, Human Rights Centre, University of Essex, available at: europa.eu.int/comm/justice_home/fsj/privacy/studies/index_en.htm.

[4] I quote a real case analysed by a consultancy firm. The pharmaceutical industry wanted to conduct scientific research using coded data collected from different hospitals located throughout the Europe. This company had to face numerous problems: was the coded data to be considered as personal data? Certain countries (NL/UK for instance) answered negatively when others were developing a broad interpretation of the notion of personal data according to recital 26 of the Data Protection Directive. Insofar as the research had been decided by the hospitals jointly with the pharmaceutical company, certain national Data Protection Authorities considered that they were together joint data controllers. In Greece, if the data collected are relative to Greek citizens as concerned persons, even if the data are processed by a company located in a different country, the Greek Law is applicable. The compatibility principle enacted by Article 6.1.b as regards scientific research is submitted to many restrictions in certain countries and not in other ones. The fact that the data transmitted were sensitive data and required the data subject's consent led to different requirements as regards the way by which this consent had to be delivered....

[5] See the two Eurobarometer surveys published by the Internal Market Directorate and available on europa.eu.int/comm/justice_home/fsj/privacy/. The first (Special Eurobarometer 196, September 2003) focuses on the views of European citizens, the second (Flash Eurobarometer 147, September 2003), on those of businesses.

privacy laws and their basic effectiveness, both for data subjects and data controllers. These polls demonstrate that, if privacy is a concern, the legal guarantees and requirements are broadly being ignored and are not, therefore, very effective. The surveys also reveal substantial discrepancies among the 15 Member States. Assessing the effectiveness of the Directive, the increasing role of the Article 29 Working Group must be highlighted. This group is an original and unique institution within the institutional European landscape. Thirdly, the article argues for new alliances to be set up by the Data Protection Authorities, so as to ensure the correct application of the provisions of the Data Protection Directive. The true judgement to be made on self-regulation, so often vaulted by business associations and encouraged by the Commission is that, unfortunately, self-regulation remains a myth. Finally, the paper examines two recent decisions of the European Court of Justice.

3.1. *Two significant Eurobarometers*

Although these new rights have been enshrined in legislation, their application remains limited, if not non-existent. As regards the Data controllers, the general feeling is described, according to the Eurobarometer's final conclusions, as follows: "No objection as such as regards the DP constraints, but the present patchwork of varying and overlapping requirements as regards information that controllers have to provide to data subjects, is unnecessarily burdensome for economic operators without adding to the level of protection".

According to the first of Eurobarometer's polls,[6] published by the European Commission in 2003, 49% of firms said that they had received fewer than 10 requests for access in 2000 and 25% said they had had none. The authors of the report on companies' perceptions of data protection legislation conclude that compliance with the law is not a priority since companies receive very few complaints. Another explanation for this relative lack of respect for Data Protection, revealed by the Eurobarometer, is the low detection risk, due to the weak enforcement measures taken by the Data Protection Authorities.[7] On that point, the situation could rapidly change due to new powers, granted to Data Protection Authorities, by most national legislations.[8]

As regards the data subjects' attitude towards Privacy issues, the second Eurobarometer survey indicates greater sensitivity among European citizens towards Privacy threats (60% compared to 25% in 1996). However, the national situations differ.[9] Notwithstanding such evolution, the Eurobarometer reveals data subjects' limited knowledge of the data protection issue and its ramifications (70% of Europeans considered that awareness of personal data protection was low) and of existing data protection legislation (only 32% had heard of the right of access, correction and erasure of data).[10] It is submitted that another factor is the relative confidence European citizens have in the measures introduced by their countries, even if they are unaware of their content. In other words, government intervention has the perverse effect of making those who should be among the first persons to be concerned – the data subjects – feel less personally responsible for their own protection.

Moreover, ordinary citizens or even their lawyers are likely to be discouraged by the abstract and excessively general wording of data protection legislation. How is an individual to interpret abstruse provisions such as one forbidding data controllers from processing data if this is incompatible with the purpose for which the data were initially collected? What should happen when he has just received an e-mail from his bank telling him that his accident insurance premium has to go up because of the additional risks arising from his recent job loss or his poor stock market investments, or that he should consider taking out a cheaper insurance with them than with a competitor, whose existence has been highlighted by a bank transfer? Many members of the public find it ironic that legislation to enable them to protect themselves and control their environment is too difficult to understand.

3.2. *The increasing role of the Article 29 Working Group*

The establishment of a consultative and independent Committee working close to the Commission that joins together representatives of the different national Data Protection Authorities, responsible for submitting advice and recommendations to the European institutions on specific privacy issues, is unique in the author's knowledge within the institutional European landscape.[11] It needs to be highlighted as a unique opportunity. Undoubtedly, the capacity of the Working Group to exercise its terms of reference in full will depend on the means at its disposal (secretary, office and the means to establish permanent common task forces at a unique location).[12]

More than 120 opinions, recommendations, resolutions on various and often important topics have been delivered by the Article 29 Working Group but beyond that visible activity, it is quite clear that the creation of this common Working Group has, to a large extent, permitted informal exchanges between the different national Data Protection Authorities. This has contributed to harmonisation in the interpretation of the provisions of the Data Protection Directive as well as an exchange of "best practices". In the context of the application of the

[6] See the two Eurobarometer surveys published by the Internal Market Directorate and available on europa.eu.int/commm/internal_market/privacy. The first (Special Eurobarometer 196, September 2003) focuses on the views of European citizens, the second (Flash Eurobarometer 147, September 2003), on those of businesses.

[7] See particularly the actions taken by the Data Protection Authorities, the survey realised by the Article 29 Working Group: "Recent examples of enforcement actions carried out by Data Protection Authorities", published as an annex of the "Article 29 Working Group Declaration on enforcement", W.P. 101, Nov. 25th, 2004.

[8] On that point, see the D. Korff's study.

[9] The Greek and Swedish public seems more anxious than the Spanish and Danish public.

[10] And only 7% had used this right of access.

[11] No similar institution is existing as regards environmental or consumer protection issues.

[12] This paper pleads strongly in favour of the creation of a "Technology Task Force" in charge of assessing new technological developments, able to give to the different Data Protection Authorities its opinion on the risks linked with them and also those present within the different standardisation organisations.

"Safe Harbour Principles"[13] a "Data Protection Panel" has been jointly created to assist European citizens. Perhaps that creation foreshadows the development of a new approach to the adoption of common positions vis-à-vis multinational or foreign companies, which will simplify their administrative tasks and harmonise the national positions. In addition to the panel, there are the various subgroups, which specialise in some of the issues creating efficiencies in the work to be done. A recent Strategy Document published by the Working Group[14] spells out its action plan. The document recognises the insufficient visibility of the Working Group vis-à-vis the Press, the difficult relationships with the EU Council of Ministers, and the need to develop an annual strategy programme. The aim is to enhance co-ordination between Data Protection Authorities to secure a better, more harmonised implementation of the Directive.

Finally, the creation and appointment of a Data Protection Supervisor at the European level needs to be flagged up. The holder of this post is responsible for ensuring recognition within EU institutions of the data protection requirements. This late creation is interesting as it may facilitate more effective co-ordination among the national D.P.A's. Overall this might lead to the development of new practices among the EU institutions setting out a blueprint for a future model for fully "privacy compliant" e-Government among the different Member States.

3.3. *New alliances*

The Eurobarometer survey has highlighted the minimal impact, to date, that Data Protection Authorities have had, often characterised by excessive legalism and procedures, rather than a genuinely active stance. This is reflected in the criticisms levelled by Flaherty[15] at an international conference of data protection commissioners: more than two-thirds of Europeans (68%) said that they were unaware of these authorities' existence and only 27% claimed to have heard references to them.[16]

This is an alarming finding. The failure of these authorities to attract media attention, even when relevant stories hit the headlines, is undoubtedly a disappointment. But a visit to their sites reveals other shortcomings. Not many are attractive,[17] and few of them allow complaints to be lodged online.[18] Only a few sites have opened discussion forums on particular themes, or have made the effort to present data protection laws in the form of frequently asked questions (FAQs).[19] There is also a regrettable absence of links to university, professional, consumer, civil liberties and other sites offering more information.[20] Nor, unfortunately, do these sites include descriptions of technological services and products offering effective protection.[21] One explanation is that financial resources may be lacking, but this may not be the only reason.

To summarise, authorities that are too inward looking need to look to other citizen protection groups with a view to offering and organising joint information and support.

Responsibility for educating data subjects and data controllers cannot be limited to Data Protection Authorities. The convergence between consumers' economic interests and citizens' freedoms opens up interesting prospects. It suggests that the right to resort to certain forms of collective action, which is already recognised in the consumer protection field, should be extended to privacy matters. Such an entitlement to "class actions" is particularly relevant in an area where it is often difficult to assess the detriment suffered by data subjects and where the low level of damages awarded is a disincentive to individual actions. Up to now, even if European Civil liberties[22] and consumer protection associations have had a part to play, they have not been very visible in the privacy debates that have occurred. Both the Commission and the Article 29 Working Group have stressed the weak reaction of this lobby in the different consultations they have organised.

Other bodies might also be cited as potential allies whose contribution should be sought, for example, Trade Union Associations which could work with Data Protection Authorities. Articles 138 and 139 of the EC Treaty impose a duty on the Commission, as regards social policy, to consult those social partners with whom agreements might be concluded. This consultation procedure has been successful in the past. An

[13] See, the EU Commission Decision 2000/520/CE about the "Safe Harbor Principles" published by the US Ministry Department of Commerce (July 21, 2000), OJCE, August 25, 2000, L. 215, p. 7 and f. On the assessment of the functioning of this Panel, see J. Dhont, M.V. Perez, Y. Poullet with the co-operation of J. Reidenberg and L. Bygraeve, *Safe Harbour Implementation Study*, Report for the EU Commission, 2004, available on the website of the Commission: europa.eu.int/comm/justice_home/fsj/privacy/. On that issue, see also, Perez Asinari, María Verónica, Poullet, Yves, "Privacy, personal data protection and the Safe Harbour decision. From euphoria to policy: from policy to regulation...?" In: *The future of transatlantic economic relations: continuity amid discord*, Florence, European University Institute, 2005, pp. 101–134.

[14] Strategy Document 29/09/04, Article 29 W.G., Working Paper, 98, 29.09.04 available on the website: europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm.

[15] David Flaherty has been Privacy Commissioner at Victoria (Canada). His criticisms against the functioning of Data Protection Authorities are broadly developed in: R.A. Grant, D. Flaherty, M. Globensky, Information Privacy: What is our responsibilities? *ICIS*, 1994, 481 pp.

[16] Only in the Netherlands, Italy and Sweden had more than one inhabitant in three heard of this authority. Under the circumstances, the Quebec approach of appointing a journalist to head the access to information and data protection commission merits further consideration.

[17] The French CNIL site is an exception.

[18] In this regard, see the various models for lodging complaints proposed by the Federal Trade Commission.

[19] See in particular the Netherlands site: www.cbpweb.nl/documenten/faq_wbp_cbp.htm and the British one: www.informationcommission.gov.uk, which also offers a particularly well constructed video and CD Rom, though unfortunately this is not available online. The French site offers a demonstration of how Net users are identified when they visit a website.

[20] Probably an indication that our authorities are anxious not to appear to be giving priority to certain opinions or institutions.

[21] Something that is offered by EPIC (Electronic Privacy Information Centre), with hyperlinks such as www.epic.org.

[22] See notably the recent creation and actions launched by the European Digital Rights Initiative (EDRI website: www.edri.org). It is a pity that the more traditional Human Rights Associations are not really present in the debate.

agreement signed by representatives of the trade unions and business associations has resulted in a framework agreement on tele-working containing different provisions on Data Protection. Data Protection Authorities can consult their social partners to produce new recommendations on data protection for employees, dealing with issues such as employees' surveillance. The product of such consultation could lead to new framework agreements.

New alliances also have to be found with companies and their administrations, particularly with the Data Protection Officials that they employ. Their experience and proximity to the real problems involved, together with knowledge of how companies have implemented privacy requirements, might be helpful in developing new and innovative solutions, seeking to balance the interests of data subjects and data controllers, while exchanging best practice. Through these links and by co-operating in educational programmes offered as a product by these associations, the Data Protection Authorities might be able to use these individuals as a means of relaying any privacy concerns. They might also become a point of contact for more effective implementation of the legislative provisions. Recently, the Article 29 Working Group has delivered an opinion,[23] recognising clearly the unique role of these individuals. There is an interest to develop a definition of European common rules on the Data Protection officials' procedure of nomination, statute and functions in order to ensure their independence.

Finally, reference is made to new jobs present in the market designed to ensure compliance with Data Protection requisites, or to assist individuals in securing their privacy needs. Infomediairies,[24] for example, are proposing added value services to fight against spam and anonymous communications or select the appropriate privacy compliant website. Labelling institutions require data controllers beforehand to affix their seal and auditing companies might be asked to certify compliance with legislative requirements. Such tasks might be better accomplished via more effective co-operation with Data Protection Authorities. There is a clear need for uniform privacy rules here.

3.4. *Self-regulation remains a myth*

Self-regulation, as an alternative to public regulation, may be a tempting prospect. Privacy policies, in the form of simple commitments indeed are flourishing. These include codes of practice and privacy standards,[25] drawn up either alone or under supervision, by the industry itself as in the case of the "Safe Harbour Principles".[26] The advantage for data subjects is that they offer principles that are adapted to the particular circumstances of a company or sector, in a language that is much easier to understand than formal legislation could impose.

The criticisms of self-regulation are well known. The first concerns the absence of safeguards regarding the effectiveness of this form of regulation. A distinction needs to be drawn here between the different types of self-regulation. Privacy commitments are undertakings by individual companies. Privacy codes of practice are laid down at more collective levels, such as within an industrial sector. Individual firms accept the principles and, in the event of non-compliance, must face any sanctions that may be imposed by the association that drew up the code. Finally, standards involve an assessment procedure for determining whether those that agree to abide by them, in fact do so. Such a procedure may take the form of certification[27] that data protection conforms to the agreed principles and the awarding of a label.[28] More general standards, subject to checks and audits, may also be developed.[29]

Remedies against non-compliance may be improved by setting up alternative dispute resolution (ADR) machinery[30] that is readily accessible, has clearly identifiable powers and is capable of producing appropriate and constructive solutions.

All these benefits and disadvantages are well known. In practical terms the procedure foreseen for promoting European Codes of conduct, with approval from the Article 29 Working Group, has been rarely followed even though clearly encouraged by the European Commission.[31] Up to now, only

[23] Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification of the role of the data protection officers in the European Union, Working Paper 106, January 18, 2005 available at: europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm.

[24] See on their potential roles in favor of Data Protection, A.DIX, "Infomediaries and negotiated Privacy Techniques", available at: www.cfp.org/paper/dix.pdf.

[25] On the difference between these forms of self-regulation see C.J. Bennett and C.D. Raab, The Governance of Privacy, Ashgate, 2003, p. 12 ff.

[26] See Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ L 215 of 25.8.2000). The Principles have been negotiated with the US government and declarations of compliance are published on the Department of Commerce official site. For the Principles as a means of joint regulation, see Y. Poullet, *Les Safe Harbor Principles; Une protection adéquate*, on www.droit-technologie.org.

[27] For example, by Trust-e, BBB Online Privacy Programme and Webtrust.

[28] See J.R. Reidenberg, *Adapting Labels and Filters for Data Protection*, Cybernews, 1997, III, 6.

[29] Examples include the Canadian Model Code for the Protection of Personal Information, approved by the Standards Council of Canada in March 1996. More recently there have been discussions in the ISO.

[30] The Safe Harbor Principles make the establishment of ADR a key element of the enforcement system: "Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved ...".

[31] See, the 2003 Commission's report and the W.G. Article 29 Strategy Document quoted, footnote 11.

two codes of conduct have been approved in that context[32] and, at national level, big disparities have been noticed. If the Netherlands, Italy and United Kingdom have been proactive, in other countries only a few codes of conduct have been enacted and these in sectors already heavily regulated (health, banking and insurance).

On the issue of self-regulatory mechanisms offering adequate protection, two comments emerge:

The recent assessment of the adequacy of protection offered by the U.S. Safe Harbor[33] provisions demonstrate the difficulty for self-regulatory systems settled upon without a legal framework. The absence of a privacy policy structure and minimum content requirement leads to a reversal of the situation. No source, for example, is identified as the publisher of this policy. Therefore, it is for the data subject to check the protection offered. Another problem concerns the difficulty of taking legal action against the non-complying data controllers. The data subject must initiate the complaint before unknown ADR institutions[34] and sometimes this must be undertaken in a foreign language. As such, this represents a major challenge. A party involved might require the intervention of the Federal Trade Commission against a US company violating its commitment, and even the Federal trade Commission might invoke such steps on the demand of US self-regulatory institutions (like BBB Online or TRUST-e or European Data Protection Authorities). The FTC's powers do not exactly fit, insofar as it is only competent to deal with privacy issues indirectly (i.e. if the privacy policy does not reflect reality or does not comply with the Safe Harbour Principles).

More recently,[35] the Article 29 Working Group has delivered an opinion on "*Binding corporate rules within multinational companies*" as a means of offering adequate protection. The Opinion underlines the importance of judging the effectiveness of the rules enacted by the multinational company. This is not only on the basis of the managerial and auditing systems that have been set up, but also the legal value of the binding rules involved. The legal recognition of the self-regulatory instruments within the Opinion needs to be underlined.

3.4.1. *When the European Judges intervene...*

Two judgements have been pronounced by the European Court of Justice on matters regarding the scope of application of the Data Protection Directive. This double intervention is quite significant. It demonstrates that judicial authority also plays a full role in the process of harmonisation. Further, the content of the decisions is noticeable insofar as the judges of the European Court of Justice are clearly asserting the full application of the Directive. In the first decision, the *Österreichisches Rundfunck* Case,[36] the question concerned whether it was legally tenable to convey information regarding the income of a civil servant to a public institution, according to a national Austrian Act. In the second decision, the *Linqvist* Case,[37] a woman working voluntarily for her local church had published on the parochial website information concerning an illness suffered by another voluntary worker. In the first case, the Court had to judge whether the Data Protection Directive, focusing on Internal Market issues, was also applicable in the case of processing undertaken by a public authority in the context of its public mission. In the second case the applicability of the Data Protection Directive to information published on a non-structured website was challenged.

The Court asserted the applicability of the Directive in both cases. The Court ruled that the Directive was to be applied as a general rule and that its non-application should represent an exception ... to be considered narrowly. In the opinion of the Court, one such exception was laid down in Article 3(2) in relation to both common foreign and security policy and police and judicial co-operation. The Court rejected the argument for so-called "minimal harmonisation" which, in the Court's opinion, contradicted the "total harmonisation" goal of the Directive. The Member States should cease departing from the commonly agreed framework achieved by the Directive.

4. The transborder data flow issues

Transborder data flow issues are clearly among the most crucial issues that the Directive has to face. The global character of the Internet requires that the protection afforded to third countries should be taken into consideration insofar as the flows are theoretically without frontiers. Articles 4, 25 and 26 of the Directive foresee an intricate system for ensuring the protection of the data collected beyond the European Union. This raises a number of delicate questions. Firstly, the

[32] The FEDMA code and the IATA code.

[33] See the Safe Harbor Analysis, V. Perez and Y. Poullet, "The New Transatlantic Agenda and the Future of Transatlantic Economic Governance: Privacy, Personal Data Protection and the Safe Harbour Decision. From Euphoria to Policy. From Policy to Regulation...?" In: *The future of transatlantic economic relations: continuity amid discord*, Firenze, European University Institute, 2005, pp. 101–134, and overall the study launched by the Commission and published at the EU Commission website: europa.eu.int/comm/justice_home/fsj/privacy/studies/index_en.htm: J. Dhont, V. Perez, Y. Poullet with the assistance of J.R. Reidenberg and L. Bygraeve, Safe Harbour Decision Implementation Study, 22 October 2004.

[34] The Safe Harbor Principles make the establishment of ADR a key element of the enforcement system. "Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved ...."

[35] Working Document on Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Working Paper 74, June 3, 2003. In 2005, the W.G. Article 29 has delivered two additional documents in order to facilitate the use of these Binding Corporate Rules.

[36] *Osterreichischer Rundfunk e.a.* ECJ May 20 2003; joined cases C-465/00, C-138/01 and C-139/01 ECR (2003) I-04989.

[37] *Bodil Linqvist* ECJ November 6, 2003, case C-101/01 ECR (2003) I-12971.

concepts used in these provisions are subject to divergent interpretations as underlined by the technical report annexed to the first review,[38] dating back to 2003. Is the notion of "transfer", for example, which is a key concept of Articles 25 and 26, opposed to the notion of "access"?[39] Technically speaking, access and transfer (push and pull) cannot easily be distinguished. What is important, with regard to such processing, is to know who has control of the information systems where the data derives. That is to say who will decide which data will be transferred? In other words, applying the Article 4c wording, can we consider that, as regards automated sending of cookies and spywares, a US company "makes use of an equipment" located in the European countries. If this is the case then, under Article 4c, European legislation is clearly applicable. In other cases, access or transfers will be subject to the conditions foreseen by Articles 25 and 26.

More precisely, the application of Article 25 assesses the adequacy of protection offered by the third country. However, a survey of national practices[40] in this regard, reveals considerable differences in approach. In certain countries the assessment is made by the data controller himself (Luxembourg), and in others by the Data Protection Authority (e.g. France and Portugal). In others still, the task is fulfilled by the Ministry of Justice (e.g. Netherlands and Sweden).

Beyond these questions, which are linked to the Data Protection Directive's provisions, it must be noted that, progressively, the European Commission, with the assistance of the Article 29 Working Group, is developing a very open framework for addressing, by different regulatory solutions (contracts, legislation, self-regulatory solutions), the multiple transborder data flow issue while complying with the World Trade Organisation's requirement for non-discrimination.[41] Article 25 requires, as a general principle, the third country to offer an adequate protection. This requires a strict interpretation of the other provisions, especially the exceptions based under Article 26.1 on the specific quality of the flow. In accordance with the methodology proposed by Working Paper no 12,[42] delivered by the Article 29 Working Group, a double assessment is required. This is based, not only on the content of the protection afforded by the third country's "regulatory" system in the broadest sense, but also upon the effectiveness of the principles so enacted. This Article 25 approach might be considered as a pragmatic and case by case solution that avoids the risk of any European "imperialism". Beyond this first solution, by adducing "adequate safeguards," (Article 26.2), the protection is no longer obtained by any external regulatory framework, such as foreseen by Article 25. Instead, it will be secured either by agreements,[43] concluded between the exporter and the importer, or by the internal decisions taken by the multinational company – the famous "Binding corporate rules".[44] By such solutions, placed at the disposal of European companies, the European Union is trying to find different ways to deal with the multiplicity of needs faced by data controllers in relation to transborder data flows.

To what extent then is it possible to speak about the Directive as a successful product for export? The answer is delicate and would need a survey of the different data flows, as well as the impact of the different solutions proposed by the Directive on these flows. Presently, no precise figures exist and it is difficult, for example, to measure the success of the Safe Harbor provisions against the more or less 600 notifications received to date by the U.S. Department of Commerce. It is also not clear to what extent any indirect influence may have been transferred by the concepts and principles underlying the Directive towards the business overseas, particularly multinational companies. Most certainly, the number of regulatory systems considered as adequate is quite limited (Argentina, US, Canada, Switzerland etc.) and certain major countries have not, up to now at least, declared their intent (China, Brazil, India, Japan, etc.). The European Union needs to be very proactive on this point insofar as the competition between privacy protection models are concerned: the European one and the US-APEC (Asia-Pacific Economic Co-operation) approach.[45] Both, it is claimed, furnish the basis for a global solution and will be subject to a major debate in the near future. It is not clear at the present time which model is likely to come out on top.

5. Towards a "techno-legal" approach: beyond the security principle

Even if each provision of the Data Protection Directive might have an impact on the design of the information systems,

[38] Technical Annex of the Analysis and impact study on the implementation of the Directive EC 95/46 in Member States Fifth annual report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and third countries: Covering the year 2000. EUR-OP, 2002. – 2 v. – ISBN 92-894-3571-2 – No. catalogue KM-39-01-001-EN-C.

[39] The distinction was one of the arguments raised in the *Linqvist* case for a non-application of the Article 25. Access to a website from foreign countries does not mean transfer. See also the PNR cases where the Article 29 W.G.' opinion distinguishes the "pull" and "push" systems.

[40] See on these points the Technical Report: Analysis and impact study on the implementation of Directive EC 95/46 in Member States, published in annex of the Review 2003.

[41] It means that the regulation imposed by a State might not interfere with possible choice for external countries to define their own way to meet the requirements enacted. See on that topic the refection proposed by Dhont, Jan, Perez Asinari, María Verónica, "New Physics and the law. A comparative approach to the EU and US Privacy and Data Protection Regulation. Looking for adequate protection", dans *L'utilisation de la méthode comparative en droit européen = Usage of methodology in European Law*, Namur, Presses Universitaires de Namur, 2003, pp. 67–97.

[42] Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive, Working Paper no. 12, July 24th, 1998.

[43] On the different contractual models, see our reflections in V. Perez and Y. Poullet, article quoted in footnote 27.

[44] On this new way to offer adequate safeguards to the Data Protection requirements in Transborder data Flows, see the Working Document (W.P. no. 74) adopted by the Article 29 Working Party on Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (June 6, 2003).

[45] See the website: www.apec.org.

a look at the Directive's provisions reveals the absence of concerns about the technology, except as regards data security. The latter issue is one of the fundamental principles and requires adoption of organisational and technical measures to protect the integrity, as opposed to the availability and confidentiality of the data in question. Since the explosion of the Internet, due to the interactive nature of the network and its large capacity, new privacy threats have surfaced. In order to face them, Data Protection Authorities have developed a more proactive policy[46] vis-à-vis the development of the information and communication technologies, either by forbidding use of technology which might jeopardise privacy,[47] or promoting technology which might assist Data Protection requirements. This might involve either incorporating privacy requirements within the infrastructure of the information systems, or including such measures within the terminal equipment itself. This "techno-legal" approach calls for closer attention to be paid to the technical aspects, as well as any positive or negative impacts that might arise in relation to the protection legally afforded to data subjects.

The Commission, in its first report on the implementation of the Directive 95/46/EC,[2] has broadly emphasised the positive role of so-called "privacy enhancing technologies" (PETs)[48] that are increasingly being cited as data protection tools. These are either as a back-up to self-regulatory approaches, such as P3P,[49] or as a substitute for other forms of regulation, for example, encryption.[50] Such approaches might be applied *to the infrastructure*, for example, the automatic blocking of connections to countries that fail to comply with data protection rules; *to data controllers or to intermediaries*, such as through the use of filters by special servers to block spam sent by certain types of enterprise; or *to data subjects' terminals*, such as through tools to either prevent the sending and receiving of cookies, or to negotiate with the data controller. Through a number of diverse research projects,[51] the Commission hopes to promote both the awareness of these solutions and the development of new tools.

Critics of such tools, whose effectiveness is acknowledged,[52] focus on the rules that apply. These rules are often agreed by experts who are not sufficiently aware of data protection requirements or are more sensitive to the needs of their industry, than to data subjects' interests. When the technologies concerned have to be applied by data subjects themselves, the *notion of user empowerment is often something of a myth*. How can individuals take responsibility for their own protection when the consequences of their decisions are not clear and when they sometimes have no choice in the matter? For example, there are sites that refuse access to users who do not accept cookies. Negotiations via P3P may be insidiously bypassed by data controllers who offer to "pay" for personal data.[53] As Dix notes[54]: "Technology is, however, no panacea for privacy risks in cyberspace; it cannot replace a regulatory framework or legislation, contracts or code of conduct. Rather it may only operate within such a framework. Privacy by negotiation is therefore no alternative to regulation, but a necessary additional tool".

Beyond these different actions, Recommendation 1/99 of the Article 29 Working Group,[55] which is concerned with the threat to privacy posed by Internet communications software and hardware, establishes the principle that such industry products should provide the necessary tools to comply with European data protection rules. This obligation, to see the data protection requirements enshrined within the development of the information systems, as asserted by the Working

[46] See the recent Working Group declaration: "New Technologies have a crucial role in promoting economic, social and human development but, at the same time, if not properly implemented, could cause adverse impact in the framework of guarantees for fundamental rights and data protection, enshrined in European Law. For that reason, the impact of new technologies on privacy has always been a prominent issue of the Working Party, as common expertise and guidance is essential in that field. Since its very early documents, there has been an ongoing interest in the relationship between emerging technologies and data protection and the Working Party has always tried to provide advice on their privacy compliant design and implementation." (Strategy Document adopted on 29 September 2004, W.P. 98.)

[47] What we call Privacy Invasive Technologies (PITs) ... like cookies, spyware, invisible hyperlinks and so.

[48] H. Burkert, Privacy Enhancing Technologies Typology, Critique, Vision, in P. Agre and M. Rotenberg (eds), *Technology and Privacy*, MIT Press, Cambridge, MA, pp. 125–143; L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999, p. 26 and ff; J. Reidenberg, Lex Informatica: the Formulation of Information Policy through Technology, 76 Texas Law Rev., 1998, pp. 552–593, Y. Poullet, Technology and Law: from Challenge To Alliance, Information Quality Regulation: Foundations, Perspectives and Applications, U. Gasser (ed.), Nomos Verlagsgesellschaft, 2004. For a presentation of PETs, see the EPIC site: http://www/epic.org/privacy/tools.html.

[49] See J. Catlett, Technical Standards and Privacy: An Open Letter to P3P Developers; on: http://www.junkblusters.com/standards.html.

[50] On the various encryption protocols and anonymous proxy servers as well as anonymisation tools and the use of pseudonyms, see C.J. Bennett and C.D. Raab, The Governance of Privacy, Ashgate, 2003, p. 148 ff.

[51] See PISA (Privacy Incorporated Software Agent), project launched in the context of the EU 5th Framework Programme which is aiming to offer an EU alternative to the P3P approach by promoting the data subjects' information and protection. On this comparison and other reflections, Borking et Raab, Laws, PETS and other Technologies for Privacy Protection, JILT, 2001, p. 1 et s (available also on the website: elj.werwick.ac.uk/filt/01-1/borking.html). See also the EU PRIME project available on the portal: www.prime-project.eu.org: PRIME elaborates a framework to integrate all technical and non-technical aspects of *privacy*-enhancing IDM.

[52] See, for example, the conclusions of the PISA project: "Privacy is probably more effective if transactions are performed by means of technologies that are privacy enhancing ... rather than relying on legal protection and self-regulation" (dbs.cordis.lu/fep).

[53] See on that point the Article 29 Working Group reflections in Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), W.P. 11, June 16, 1998.

[54] A. Dix, Infomediaries and Negotiated Privacy Techniques, paper presented at the conference "Computers, Freedom and Privacy" (CPF 2000), 19 April, Toronto, on: http://portal.acm.org/citation.

[55] Recommendation on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware.

Group, has been emphasised in its recent recommendation[56] about Radio Frequency Identification technology (RFID). Article 14 of the Directive 2002/58/EC states that, where required, the Commission may adopt measures to ensure that terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is another, admittedly subsidiary way, of protecting personal data from the risks of unlawful processing – risks that have been created by these new technological options.

To become involved into the standardisation process is another concern of the Article 29 Working Group.[57] In 2004, at the 26th International Conference of Privacy and personal data Protection, held at Krakow, the final resolution emphasised the need for Data Protection Commissioners to work jointly with standardisation organisations to develop privacy related technical and organisational standards.[58] The recent CEN and ISO standards on security and privacy[59] are certainly a first step in that direction. However, Data Protection Authorities must play their part in the debate, which is currently taking place among private standardisation bodies such as Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN) and World Wide Web Consortium (W3C).

6. The Directive facing new conflicts of values

Article 9 of the Data Protection Directive enunciates the principle of establishing the right balance between data protection and freedom of expression. This delicate balance is challenged in three directions. The first relates to the problem of equilibrium between the requisites of data protection and freedom of information legislation. The latter seeks greater governmental transparency and is considered as a tool to ensure freedom of expression within the limits to that transparency imposed by data protection regulation. Usually a single institution is charged with responsibility to define this equilibrium. This trend is a very positive one insofar as, in most cases, the central issue is the right of every citizen to enjoy self-determination within the information society. The second question concerns electronic journalism. Ordinary citizens are more and more frequently using user-friendly technology (like Internet websites or blogs) to disseminate their opinions on societal events. At issue is whether these new forms of journalism can enjoy the different exceptions introduced within national legislation to protect journalists? Finally, there is the risk of abusive extensions to Data Protection legislation that might be detrimental to freedom of expression. In the *Linqvist* case, already quoted,[60] the European Court of Justice argued that any Internet website containing personal information was subject to privacy legislation, even if the data were not structured and were without metatags. It is submitted that this trend is quite dangerous insofar as an individual is, by essence, located in a society and within a variety of relationships with other people. The duty not to mention such relationships, or to adhere to any limitations imposed when referring to them, has to be viewed as an illegitimate restriction on the freedom of expression.

On the question of the balance between public security interests and privacy related ones, the events in 2001 on 11th September have provoked fundamental debate. It must be recalled that, just six days before these sad events, the European Parliament severely criticised the US–UK *Echelon Programme*[61] for creating an illegal surveillance system in breach of Article 8 of the Council of Europe Convention. Since then, the fight against terrorism has been used to justify new investigatory powers, which might be questioned from a privacy perspective. The access to Passenger Name Records[62] requested by foreign countries and the traffic data retention

[56] "In this context, Working Party 29 wishes to emphasize that while the deployment of an RFID application is ultimately responsible for the personal data gathered through the application in question, manufacturers of RFID technology and standardization bodies are responsible for ensuring that data protection/privacy compliant RFID technology is available for those who deploy the technology. Mechanisms should be developed in order to ensure that such standards are widely followed in practical applications. In particular, RFID privacy compliant standards must be available to ensure that data controllers processing personal data through RFID technology have the necessary tools to implement the requirements contained in the Data Protection Directive. The Working Party therefore urges manufacturers of RFID tags, readers and RFID applications as well as standardization bodies to take the following recommendations into account." (Opinion of the Article 29 W.G. – Opinion 19.01.2005, already quoted).

[57] See as regards this concern, the Article 29 Working Group Opinion 1/2002 on the CEN/ISSS Report on Privacy Standardisation in Europe, W.P. 57, May 30, 2002.

[58] Whereas the International Conference wishes to support the development of an effective and universally accepted international privacy technology standard and make available to ISO its expertise for the development of such standard.... Final resolution of the 26th International Conference on Privacy and Personal Data Protection (Wroclaw, September 14, 2004). Resolution on a draft ISO Privacy standards).

[59] The Security and Privacy Standards TC is a P member in ISO/IEC JTC1/SC27 – Security Standards. For more details on the ISO action on that field, see the website: www.itsc.org.sg/TC/5th_term_compo/spstc.html. Read also, the CEN/ISSS secretariat Final Report: "Initiatives on Privacy Standardization in Europe", Febuary 13, 2002, available at: www.europa.eu.int/comm/enterprise/ict/policy/standards/ipsc_finalreport.pdf.

[60] See supra no. 21.

[61] In 1998, a European Parliament report published by the STOA (Scientific and Technological Options Assessment): "Appraisal of Technologies control" (see particularly, D. CAMPBELL, Development of Surveillance Technology and Risk of Abuse of Economic Information available at: www.Europarl.int/stoa/public/pdf/98-14-01-2en.pdf) alerted European opinion to the existence of a network called ECHELON, run by the English, American, Canadian, New Zealand and Australian secret services, capable of capturing and analysing all messages passing through geostationary satellites. This report leads to the Resolution no. 15 adopted by the European Parliament (September 5, 2001), which "urges the Commission and Member States to develop appropriate measures to promote and manufacture European encryption technology and software" in order to protect privacy and the economic interests of the European countries.

[62] On that issue, see M.V. Perez Asinari – Y. Poullet, "The airline Passenger data disclosure case and the EU–US debates", in CLSR, 2004, no. 19, pp. 61–65 and "Airline passengers' data adoption of an adequacy decision by the European Commission. How will the story end?" In: CLSR, 2004, no. 20, pp. 370–376.

by law enforcement authorities, raise further sensitive questions about the frontier between the first and the second or third pillars of the Treaty on European Union.[63] This requires an extension of the principles, enacted in the 1995 Data Protection Directive, from the first pillar to the other pillars' activities.

The development of e-Government also arouses new concerns regarding the traditional balance between the functions of administrations and the citizens' liberties. New tools, for example, are at the disposal of the authorities (electronically readable identity cards, official e-signature, referential data bases). Moreover, its operations are increasingly based on networks to ensure circulation of information between the separate departments.[64] These trends are occurring within government, generally for a multiplicity of reasons, but nevertheless "big brother" fears are raised. It is not sufficient that technical or organisational methods are available to ensure equilibrium exists between the two potentially conflicting interests. The public is generally quite in favour of these new e-Government applications, insofar as they facilitate better administrative and governmental procedures. Data Protection Authorities hence have difficulty justifying their opposition to such "progress'. So, as regards the multiple developments of e-Government applications, it is more and more up to Data Protection Authorities to outline their objections to these developments. It is not simply a question of public authorities seeking to justify, according to the proportionality principle enacted within Article 8.2 of the Council of Europe Convention on Human rights, why the public interest should override the concerns of the individual towards confidentiality. According to Article 8.2 of the European Convention on Human Rights (ECHR), it should normally be for administrations to establish which superior concerns might justify necessary limitations on privacy and not for the public to raise privacy concerns arising directly from the e-Government agenda.

7. Towards a third generation of Data Protection legislation: a multilayer approach

Since 1995, the EU has adopted two major instruments concerning data protection. The first is the EU Charter of Fundamental Rights[65] and the second, Directive 2002/58/EC on Data Protection in the communications sector. The thesis of this paper is that, through these texts, the original concept of privacy is becoming overwhelmed by new approaches which go far beyond the scope of the protection enacted originally by Article 8 of the 1950 ECHR. This does not mean that the initial concept should be forgotten, but that new layers of protection need to be added to the initial one.

Article 8 of the ECHR has the essential task of protecting the individual against arbitrary interference by the public bodies in his/her private or family life. With regard to the basic ambit of the right to respect for private life, this might be understood as being limited to a minimal sphere, defined both as a physical sphere (the family home) and a communication sphere (e.g. mail services and voice telephony) within which he/she can freely pursue the development and fulfilment of the personality – perhaps a prerequisite for a person's dignity. This is a negative interpretation as it can be translated as an instruction for public authorities to violate this sphere of intimacy.

The point of departure of the Directive (and of the Council of Europe Convention no. 108[66]) is totally different and constitutes a second approach. The main aim is to grant subjective rights in favour of the data subject, so as to allow the individual to exercise control over the information concerning his or her person (right to be informed, right to access, right to rectify, etc.). These subjective rights might be considered as a counterbalance (and control mechanism) for the increasing informational powers provided by ICT to data controllers. The protection is thus no longer linked to a physical or "communicative" space, but embraces all personal data. This protection necessarily implies certain limitations to the collection, processing and disclosure of personal data in order to maintain a balance between protecting the liberties of the data subject and the legitimate interests of data controllers. This balance has to be achieved under the control of an independent authority.

The need to distinguish clearly between the first approach, based on the defence of privacy and the second one, that of increasing protection of personal data, has led to the grant of new rights, limiting the prerogatives of data controllers and installing a means to keep the balance. This approach has now been brought into being by the EU Charter of 2000.[67] Article 7 recalls the content of the initial Article 8 ECHR, while Article 8 of the Charter enacts a new complementary right: the right to Data Protection. This fundamental text, which does not present any direct mandatory rules, might be considered as a first attempt to define constitutional rights for the

[63] The activity of the EU is usually illustrated by three pillars. The first pillar is composed of the European Communities, and basically consists of traditional co-operation within the European Community. It covers matters pertaining to the Single Market and the "four freedoms', that is, free movement of persons, goods, services and capital across borders. Community co-operation also includes matters related to agriculture, the environment, competitiveness and trade policy. The first pillar also includes co-operation in fiscal and monetary issues, i.e., the development of the Economic and Monetary Union (EMU). The second pillar consists of the Common Foreign and Security Policy (CFSP). The third pillar comprises police co-operation and co-operation in the area of criminal law. The role of the European Parliament is less important as regards decisions taken in the context of the two last pillars, decisions which require the unanimity of the Member States.

[64] This traditional separation between the different departments or administrations was traditionally viewed as a fundamental guarantee for ensuring the protection of the individuals.

[65] EU. Charter on Fundamental rights (adopted at Nice, December 18, 2000) published in the O.J. of the European Communities, Declaration 2000/C 364/01.

[66] Council of Europe Convention no. 108 on the protection of Individuals against the automated treatment of personal data, adopted by the Council of Ministers, January 28, 1981.

[67] This Charter has been enacted by the Treaty of Nice (O.J. c80, March 10, 2001). The text is available at the website of the European Commission – Justice and Home Affairs: www.eu.int/comm/justice_home/unit/charte/index_en.html.

European citizen, as it includes two provisions concerning data protection. Article 7[68] is more or less a copy of Article 8 of the ECHR. It protects family life, domicile and enacts protection for private communications. This is translated into the traditional conception of privacy as a defence against intrusion. Curiously, Article 8 establishes a distinct Human right: the right to data protection. This must be considered, apart from the Treaty, as a human right separate and complementary to the concept of privacy itself. Article 8[69] reasserts the four major principles of all data protection law. The First principle establishes that all personal data, not only sensitive data, are to be covered by this new human right. Secondly, new subjective rights are to be granted to data subjects to access and to rectify erroneous data. Thirdly, certain limitations are imposed upon data controllers, for example, the fair collection of data and data quality. Fourthly, in order to balance the interests and liberties of data controllers, against those of data subjects, specific reference is made to the role of the Data Protection Authority. The draft E.U. Constitution,[70] still being debated at the European level, takes again these two provisions.

It is submitted that Directive 2002/58/EC[71] constitutes a third approach. It takes into account, in the context of modern networks, the possible existence of a third actor operating between data controllers and data subjects. This is the technology – a more and more complex infrastructure, with new visible and invisible actors, as well as terminal equipment (e.g. personal computers, mobile phones and RFID) able to act independently of the "consciousnesses of their possessors. Even if its wording remains ambiguous, the Directive takes this new environment into account and goes beyond the scope of the General Data Protection Directive. Traffic and location data are regulated, even it is unclear whether they are considered as personal data. Quite clearly, it is not so much the protection of an identified or identifiable person that is looked for, but the fact that the possession of a terminal will permit certain actions to be performed vis-à-vis a person, even if that person is not, as such, identifiable. The protection of the right to self-determination implies regulation of the use of data concerning objects, and is not only relative to persons as it was via the second approach. Certain provisions of the Directive on data protection in the electronic sector impose new duties and new data processing limitations to certain actors, independently of the quality of data controllers. For example, Internet access providers and communication infrastructure operators are subject to strict limitations as regards the processing of traffic and location data. At the same time they are required to co-operate with law enforcement authorities. Finally, a most notable point is the nascent regulation of terminal equipment, which must be compliant with data protection requirements[72] and be configured in a way which does not allow illegal uses of the user's information systems.[73]

8. Conclusions

To conclude this evaluation of 10 years of the existence of the Data Protection Directive, certain reflections are called for in relation to Data Protection Authorities.

The first derives from the increasing competence given to such bodies by Article 28 of the Directive. According to the European text, most Member States have given their equivalent organisations investigative powers and jurisdictional competences. Consequently, the Authorities are permitted to deliver injunctions and authorisations. These new statutory competences radically modify the functions, the statute and the sense of the Authorities' action. Indeed, with their consultative powers, it was easy for them to be in a "lobby position" that Flaherty designated as a "watchdog function" 20 years ago. But these new responsibilities imply the adoption of a role of neutral "balance keeper", avoiding any "*parti pris*', which might otherwise create the risk of the kind of administrative response already criticised by Flaherty. It is submitted that Data Protection Authorities should carefully protect their privacy minded approaches and not forget to apply them at the right moment. DPA's need to recall their positive obligation upon government to respect constitutional rights to privacy. This means, inter alia, developing at the appropriate level (e-Government applications) best practices which might serve as an example for business activities.

A second point appears to be quite important in this respect. The fight to maintain data protection needs to go beyond the legal discussion and those restricted circles where these questions are classically discussed. The authorities have to find new allies, including data controllers, as well as new services to serve the market. They have to participate in new environments too, particularly among the standardisation

[68] Article 7: "Everyone has the right to respect for his or her private and family life, home and communications".

[69] Article 8: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".

[70] See Articles II-67 and II-68 of the EU Draft Treaty establishing a *Constitution* for Europe, adopted by consensus by the European Convention on 13 June and 10 July 2003, submitted to the President..., available at www.eu.int/futurum/constitution/index_en.html.

[71] The Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector replaces and modifies quite significantly the provisions of the former Telecommunications Data Protection Directive 97/66/EC insofar as it intends to take fully into account the Internet environment. Even it is asserted that the new Directive is just particularising and completing the General Data Protection Directive, it might be underlined that the new instrument is enlarging considerably the scope of the previous data protection texts by including a protection of the legal persons, by going into much more on concepts related to the conservation and use of location and traffic data and by tackling the issue of unsolicited e-mail. Furthermore, it imposes new obligations to Internet access providers and publicly available networks' operators. Finally, it creates a possibility to impose standards to the terminal equipments' manufacturer in order to ensure their privacy compliance.

[72] See Article 14 of the Directive 2002/58/EC and our reflections above no. 28.

[73] See Article 5.3 of the Directive.

bodies, and take the technology issues and challenges seriously into account. On that point they have to develop the means to engage in "technology assessment" and apply the "precautionary principle"[74] in full, as is the case with environmental questions. The openness of Data Protection Authorities to these societal and technological contexts is the only chance available for preserving the right to self-determination in the global information society. That success will depend, in part, on a constructive interplay between Data Protection Authorities and the press.

As a final point, it is submitted that Directive 95/46/EC represents the most constructive means, yet devised, for defending our liberties. If Data Protection Authorities want this model to be followed at a global level, they will need to act jointly to ensure that effective harmonisation takes place in respect of privacy requirements among the different jurisdictions. They must also avoid excessive administrative charges, by creating unique gateways. Common services, such as an agency to deal with techno-legal questions (promotion of PETS,[75] assessment of new technological products, etc.) would be useful. There also needs to be promotion, at European level, of self-regulatory solutions which might easily be extended to other countries. The newly created European Data Protection Supervisor might play a fruitful role in that context. In short, it is now time to blow out the candles and to offer the Directive a resounding "Happy Birthday"!

Professor Yves Poullet, (yves.poullet@fundp.ac.be), Director Crid, University of Namur, Belgium; http://www.crid.be.

[74] "The precautionary principle, a phrase first used in English circa 1988, is the idea that if the consequences of an action are unknown, but are judged to have some potential for major or irreversible negative consequences, then it is better to avoid that action. The principle can alternately be applied in an active sense, through the concept of 'preventative anticipation', or a willingness to take action in advance of scientific proof of evidence of the need for the proposed action on the grounds that further delay will prove ultimately most costly to society and nature, and, in the longer term, selfish and unfair to future generations. In practice the principle is most often applied in the context of the impact of human civilization or new technology on the environment, as the environment is a complex system where the consequences of some kinds of actions are often unpredictable. The formal concept evolved out of the German socio-legal tradition that was created in the zenith of German Democratic Socialism in the 1930s, centering on the concept of good household management. In German the concept is Vorsorgeprinzip, which translates into English as precaution principle. The concept includes risk prevention, cost effectiveness, ethical responsibilities towards maintaining the integrity of natural systems, and the fallibility of human understanding." (en.wikipedia.org/wiki/Precautionary_principle).

[75] By comparison, it is quite interesting to see on the US NGO EPIC website (www.epic.org/privacy/tools.html) comments and hyperlinks about PETS products, which might be helpful for the data subjects. Why our Data Protection Authorities are not offering the same services?